Europ. J. Combinatorics (1989) **10**, 189–196

A Lloyd Theorem in Weakly Metric Association Schemes

PATRICK SOLÉ

Weakly metric association schemes are a generalization of metric schemes occurring in graph theory (vertex transitive digraphs), coding theory (Lee scheme, Clark–Liang scheme), and group theory (conjugacy scheme).

Linear constraints on the inner distribution of r-covering codes in these schemes lead to a 'Lloyd theorem' on perfect codes. This generalizes results from Delsarte, Biggs, Bassalygo and Landauer.

1. INTRODUCTION

Issued from coding theory [12, 19], the fascinating problem of the existence of perfect codes was drawn into the realm of graph theory by Biggs [4], who set it in the framework of distance-transitive graphs. At the same time, independently, it was set by Delsarte in the more general context of distance-regular graphs [7], or equivalently metric association schemes. Bassalygo investigated the case of codes for the Lee distance [3]. We recovered his results in the context of the Lee scheme [13]. A connection was recently established, by Etienne [18], with the work of Landauer in group theory [10].

In every case there was a theorem related with an old result of Lloyd [11]. We give a general version of this theorem, which encompasses all previously known versions, and leads to new results (see sections 7.3 and 7.4). The ingredients of the proof are Stanton–Kalbfleisch inequalities (section 5), which appeared (in special cases) in recent work [6] on covering radius, and a lower bound on external distance (section 4), which generalizes the MacWilliams inequality of metric schemes [7] to weakly metric schemes [15].

2. WEAKLY METRIC SCHEMES

2.1. DEFINITIONS. A *commutative association scheme with t classes* (X, R) consists of a finite set X, along with a partition $R = (R_0, R_1, \ldots, R_t)$ of X^2 satisfying the following axioms:

A_0: $R_0 = \{(x, x)/x \in X\}$.

A_1: $(R_i)^{-1} = \{(y, x)/(x, y) \in R_i\} = R_{i'}$ for some i' in $[0, \ldots, t]$.

A_2: $\forall (x, y) \in R_k | \{z/(x, z) \in Ri$ and $(z, y) \in Rj\}| = p_{ij}^k$.

A_3: $\forall (i, j, k) \in [0, \ldots, t]^3 p_{ij}^k = p_{ji}^k$.

If A_1 is replaced by $(A_1)'(R_i)^{-1} = R_i$, then (X, R) is said to be *symmetric*.

We call *quasi-distance* on X any mapping from X^2 to the non-negative reals satisfying the triangle inequality. Furthermore, if this mapping is symmetric, it is called a *distance*.

We consider a commutative association scheme with t classes (X, R) [2], equipped with a quasi-distance d constant on the classes of the scheme:

$$\forall (a, b) \in X^2 a R_k b \Rightarrow d(a, b) = d(k).$$

We call such a scheme *weakly metric* for the quasi-distance d. Clearly, all metric schemes [7] are weakly metric for the shortest path distance on the Γ_1 graph with $d(k) = k$.

0195-6698/89/020189+08 $02.00/0

2.2. Examples

2.2.1. Vertex-transitive Digraphs. Let Γ be a simple vertex-transitive digraph with automorphism group G. If we let X be the vertex set of Γ and R be the partition of X^2 into orbits under the action of G, then (X, R) is an association scheme [2], which is weakly metric for the shortest path distance on Γ. If we assume that G is generously transitive [2], then (X, R) is symmetric. It can be shown [16] that the two following examples satisfy this pattern in the symmetric case, and the third in the non-symmetric case. The fourth example is different.

2.2.2. The Lee Scheme. We define the Lee composition of any z in $(Z_q)^n$ as the $s+1$-tuple $lc(z)$ such that

$$c_i = |\{j = 0, 1, \ldots, n/z_j = \pm i\}|.$$

The Lee scheme [1, 18] on $(Z_q)^n$ is defined by the relations: $xR_k y$ iff $lc(x-y) = k$, where k runs over the possible composition vectors. This scheme is denoted by $L(n, q)$ [18].

The Lee distance [12] is defined by the following: if $xR_k y$ then $d(x, y) = k_1 + 2k_2 + \cdots + sk_s$, where $k = lc(x-y) = (k_0, k_1, k_2, \ldots, k_s)$.

All this shows that $L(n, q)$ is weakly metric for the Lee distance.

2.2.3. The Clark–Liang Scheme. We let $X = Z_M$ and d be the modular distance with radix r [19, 15]. If $(r, M) = 1$ the multiplicative group generated by r and by -1 acts on Z_M with orbits X_k and we defined in [15] the following scheme:

$$xR_k y \Leftrightarrow x - y \in X_k,$$

This scheme is weakly metric for the Clark–Liang distance, and is a natural setting for the study of arithmetic codes for this distance [15, 17].

2.2.4. The Conjugacy Scheme. Let G be a finite non-abelian group, and $C_0 = \{1\}, C_1, \ldots, C_t$ its conjugacy classes. We can define an association scheme on G [7], [2] by the relations:

$$xR_i y \Leftrightarrow xy^{-1} \in C_i.$$

We call it the *conjugacy scheme* on G. It is symmetric iff every C_i is *real*, i.e., $C_i = C_i^{-1}$.

Take for d any quasi-distance which is *bi-invariant* [5]:

$$\forall (x, y, z) \in G^3 d(xz, yz) = d(x, y) = d(zx, zy).$$

Then (G, R) is weakly metric for d. For instance, we can consider the Cayley graph on G, with edge set $E = \{(x, y)/xy^{-1} \in H\}$, where H is the union of non-trivial conjugacy classes. We call $\mathscr{H}$ the set of these classes. The shortest path quasi-distance on this graph is bi-invariant.

A rather different example is for $G = S_n$ and $d(\sigma, \tau) = |\{\text{moved points of } \sigma\tau^{-1}\}|$, [5]. This distance does *not* stem from a graph [14], since there is no pair of points at distance 1 of each other.

3. Perfect Codes

Let Y be a non-empty subset of X. Y is called a code. A code is said to be an r-covering if

$$\forall z \in X \; \exists y \in Y \; d(z, y) \leqslant r.$$

The largest r such that Y is an r-covering is called the *covering radius* of Y. In an analogous way we define the *packing radius* e as the largest integer j such that the balls of radius j are disjoint.

Note that in a weakly metric scheme all balls of radius j have the same volume, say b_j:

$$b_j = \sum_{d(i) \leqslant j} v_i,$$

where the v_i are the valencies of the scheme [2].

If Y is an r-covering, then we have the natural counterpart of the covering bound in $H(n, 2)$ [6]:

$$|X| \leqslant |Y| b_r.$$

Codes meeting this bound with equality are said to be *perfect* and have the property that $r = e$.

4. The External Distance of a Code

Let Y be a code in the weakly metric scheme (X, R). We define its *inner distribution* by

$$a_i = (1/|Y|)|R_i \cap Y^2|; \qquad i = 0, 1, \ldots, t.$$

In a metric scheme this is the distance distribution; in $L(n, q)$ the Lee composition distribution [12].

The *dual* inner distribution is defined consistently with (7) by

$$a'_k = \sum_{i=0}^{t} a_i Q_k(i),$$

where the $Q_k(i)$ are numbers depending on the scheme and called *second eigenvalues*. There is an inversion formula:

$$a_k = \frac{1}{|X|} \sum_{i=0}^{t} a'_i P_k(i)$$

where the $P_k(i)$ are numbers depending on the scheme and called *first eigenvalues*.

We call *external distance* of the code Y and denote by s' the number of non-zero a'_i for $i \geqslant 1$.

In a weakly metric scheme (X, R) for the distance d, we define the *dispersion function* Π: $\Pi(j) = |\{i/d(i) \leqslant j\}|$. Π measures the 'non-metricity' of the scheme.

We shall need the following result from [14, 15]:

Theorem 1. *For every code Y of packing radius we have $s' \geqslant \Pi(e) - 1$.*

In the particular case of a metric scheme this is the *macWilliams inequality* [7, 12]: $s' \geqslant e$.

5. Inequalities for r-Coverings

5.1. Linear constraints on the inner distribution of a set. Let Y be a subset of X, x a point of X, and $A_k(x)$ the number of Y k-related to x. The inner distribution of Y is easily seen to be:

$$a_k = \left(\sum_{x \in Y} A_k(x)/|Y| \right).$$

PROPOSITION 1. *Necessary conditions for Y to be an r-covering are*:

$$\forall x \in X, \quad \forall i \in [0 \cdots t]: \sum_{d(i)-r \leqslant d(k) \leqslant d(i)+r} A_k(x) \left(\sum_{d(j) \leqslant r} p_{ij}^k \right) \leqslant p_{ii'}^k.$$

COROLLARY 1. *Necessary conditions for Y to be an r-covering are*:

$$\forall i \in [0 \ldots t]: \sum_{d(i)-r \leqslant d(k) \leqslant d(i)+r} a_k \left(\sum_{d(j) \leqslant r} p_{ij}^k \right) \geqslant p_{ii'}^k.$$

PROOF. Let us consider the set $X_i(x)$ defined by

$$X_i(x) = \{z \in x / z R_i x\}.$$

The definition of the intersection number yields

$$|X_i(x)| = p_{ii'}^0 = v_i.$$

Now, any z in this set is at most r away from some y in Y, so that there exists an index j such that

$$z R_j y \tag{2}$$

and

$$d(j) \leqslant r.$$

Such a y is k-related to the 'origin' x and, according to the triangle inequality,

$$|d(i) - r| \leqslant d(k) \leqslant d(i) + r.$$

Then, by definition of the intersection numbers p_{ij}^k and of $A_k(x)$, the l.h.s. of equation (1) counts the number of such y. Since the correspondence $y \leftrightarrow z$ is many-to-one, the l.h.s. is greater than the r.h.s.

The corollary follows immediately by averaging equation (1) over x in Y. QED.

EXAMPLE 1. In $H(n, 2)$ this specializes to the Stanton–Kalbfleisch inequalities [6]. For $r = 1, 2$ this yields:

$$(n - i + 1)A_{i-1} + A_i + (i + 1)A_{i+1} \geqslant \binom{n}{i},$$

$$\binom{n - 1 + 2}{2} A_{i-2} + (n - 1 + 1)A_{i-1} + (1 + in - i^2)A_i + (i + 1)A_{i+1}) + \binom{i + 2}{2} A_{i+2} \geqslant \binom{n}{i}.$$

This is easily recovered by using the generating function for the intersection numbers of $H(n, q)$:

$$\sum_{i,j} p_{i,j}^k x^i y^j = [x + y + (q - 2)xy]^k [1 + (q - 1)xy]^{n-k}. \tag{3}$$

Equation (3) occurs in computing false decoding probability estimates [9].

5.2. EQUALITY IN THE CONSTRAINTS. We recall that a set Y is fulfilling the covering bound with equality iff Y is perfect.

PROPOSITION 2. *The constraints on the inner distribution of Y are fulfilled with equality iff Y is perfect.*

PROOF. These conditions are realized iff the correspondence $y \leftrightarrow z$, defined in (2), is one-to-one, which means that the balls of radius r centered on the points of Y pack the space X. QED.

An application of this result is an elementary proof [16] that the distance distribution of a perfect code in a metric scheme is uniquely determined by its parameters [7].

6. A LLOYD THEOREM IN WEAKLY METRIC SCHEMES

6.1. THE INTERSECTION ALGEBRA. In a scheme with t classes on X, we consider the $t + 1$ matrices with complex entries indexed by $[0, \ldots, t]^2$ and defined by:

$$B_j(i, k) = p_{ij}^k.$$

The well known relation

$$P_i(l)P_j(l) = \sum_{k=0}^{i} p_{ij}^k P_k(l)$$

yields

$$P_j(l)P_i(l) = \sum_{k=0}^{t} B_j(i, k)P_k(l).$$

We denote by $\mathbf{v}(l)$ the columns of the matrix P:

$$\mathbf{v}(l) = (P_0(l), P_1(l), \ldots, P_t(l))^{\mathrm{T}}.$$

From the preceding computation we have that $\mathbf{v}(l)$ is a right eigenvector of matrix B_j associated with the eigenvalue $P_j(l)$:

$$B_j\mathbf{v}(l) = P_j(l)\mathbf{v}(l).$$

Note that the algebra spanned over the complex field by the B_j is isomorphic to the Bose–Mesner algebra of the scheme [2].

6.2. DIAGONALIZING THE CONSTRAINTS. We introduce the Lloyd polynomial:

$$\Psi_r(l) = \sum_{d(k)\leqslant r} P_k(l).$$

When the scheme is metric it is a polynomial in the single variable $P_1(l)$. In the general case it is a polynomial in g variables $P_{i_1}(l), \ldots, P_{i_g}(l)$, where the adjacency matrices $D_{i_1}, \ldots, D_{i_g}$ span the Bose–Mesner algebra of the scheme.

For instance, in the case of $L(n, q)$, it is a polynomial in $[q/2]$ variables [19, 24].

THEOREM 2. *Let Y be e-error correcting. Then $\Psi_e(l)$ vanish for at least $\Pi(e) - 1$ values of l.*

PROOF. We define the Lloyd matrix as:

$$L_j = \sum_{d(i)\leqslant j} B_i.$$

From the preceding section $\mathbf{v}(l)$ is a right eigenvector L_j associated to the eigenvalue $\Psi_j(l)$:

$$L_j \cdot \mathbf{v}(l) = \Psi_j(l)\mathbf{v}(l).$$

If Y is perfect we have equality in the constraints which, together with

$$a_k = \frac{1}{|X|} \sum_{i=0}^{t} a_i' P_k(i),$$

yields

$$\frac{1}{|X|} \sum_{i=0}^{t} a_i \Psi_e(i) \mathbf{v}(i) = \mathbf{v}(0).$$

Since P is non-singular the $\mathbf{v}(i)$ are linearly independent and we obtain:

$$a_i' \Psi_e(i) = 0, \qquad i = 1, \ldots, t.$$

(The case $i = 0$ simply yields the equality in the covering bound.) This implies:

$$(i \geqslant 1 \text{ and } a_i' \neq 0) \Rightarrow \Psi_e(i) = 0.$$

Now we make good use of the MacWilliams inequality (Theorem 1), and we are done. QED.

In the slightly less general context of vertex-transitive digraphs one can prove a stronger result. Define the primal Lloyd matrix as:

$$PL_j = \sum_{d(i) \leqslant j} D_i.$$

THEOREM 3. *A necessary condition of existence of a perfect code of covering radius e is*:

$$\dim(PL_e) \geqslant b_e - 1.$$

SKETCH OF PROOF. We fix an origin y in the perfect code Y. For every a in the ball of radius e centered in y there is an automorphism of the digraph which maps x on a. We denote by Y_a the image of Y under this map.

A well known necessary condition [4, 8] for Y to be perfect is:

$$PL_e \cdot \phi_Y = \phi_X$$

where ϕ_Z denotes the characteristic function of the set Z. Since the Y_a are perfect, the vectors $\phi_{Ya} - \phi_Y$ are in the kernel of PL_e. They are linearly independent, for their supports are disjoint. QED.

7. APPLICATIONS.

7.1. METRIC SCHEMES. If d is the shortest path distance on a distance-regular graph, and (X, R) the associated P-polynomial metric scheme, then $d(i) = i$, $i = 0, 1, \ldots, t$, where t is the diameter of the graph, and we recover immediately the expression of Lloyd polynomial and Lloyd theorem in metric schemes [7].

Note that our results also apply to *distance-regular digraphs* [2], which seems to be new.

7.2. THE LEE SCHEME. Using the multivariate generating function of the first eigenvalues given in [13, 1], the result of Bassalygo [3] is recovered.

7.3. THE CLARK–LIANG SCHEME. Using the fact that the scheme is abelian [16], its eigenvalues can be computed, at least numerically. Our results are technical, and will be published elsewhere [17].

7.4. THE CONJUGACY SCHEME. A perfect code of covering radius 1 is exactly a perfect H-code in the sense of Etienne [8]. The first eigenvalues of the conjugacy scheme are:

$$p_i(\chi) = (|C_i|/d_\chi)\chi(C_i),$$

where χ is an irreducible character of G, of degree d_χ [7, 2].

It is easily checked that $\Pi(1) = 1 + |\mathscr{H}| = 1 + s$ in the notations of [8], and that

$$\Psi_1(\chi)) = 1 + \sum_{d(i)=1} (|C_i/d_\chi)\chi(C_i) = 1 + \sum_{K\in\mathscr{K}} (|K|/d_\chi)(K).$$

We denote by N the set of irreducible characters of G which cancel Ψ_1.

We recall and prove the result of Landauer, [10], cited in [8].

THEOREM 4. *If there exists a perfect H-code then*:

$$(i) \sum_{\chi\in N} (d_\chi)^2 \geqslant |H|;$$

$$(ii) |N| \geqslant s.$$

SKETCH OF PROOF. The condition (ii) is a direct consequence of Theorem 2 and condition (i) of Theorem 3 modulo the computation of its l.h.s. (see [8] for details). QED.

Our results are stronger, since they also include the case of perfect codes of covering radius $e > 1$.

8. SOME OPEN PROBLEMS

(1) If Y is a perfect code, does it always hold that $s' = \Pi(e) - 1$? The converse is true [15].

(2) Is it possible to generalize the concept of regular partition [8] in our context?

(3) Are the properties of multivariate orthogonal polynomials of any help in establishing non-existence theorems?

(4) Are there perfect codes in distance-regular digraphs, other than the trivial ones in directed cycles of even order?

REFERENCES

1. J. Astola. The theory of Lee codes, Lapperanta University Research report, 1982.
2. E. Bannai and T. Ito, *Algebraic combinatorics I: Association schemes*, Benjamin Cummings, Menlo Park, 1984.
3. L. A. Bassalygo, *math. Zametki*, **15** (2) (1974), 313–320 (in Russian).
4. N. Biggs, Perfect codes in graphs, *J. Combin. Theory*, **15** (1973) 289.
5. G. Cohen and M. Deza, Distances invariantes et L-cliques sur certains demi-groupes finis, *Math. Sci. Hum.*, **69** (1975), 49.
6. G. Cohen, A. Lobstein and N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inform. Theory*, **32** (1986), 328–343.
7. P. Delsarte, Thesis, Phillips Research Supplements 10, 1973.
8. G. Etienne, Perfect codes and regular partitions in graphs and groups, *Europ. J. Combin.*, **8** (1987), 139–144.
9. S. Jennings, On computing the performance probabilities of Reed Solomon codes, *Proc. AAECC03*, J. Calmet, ed., Springer Verlag, Berlin–Heidelberg–New York, 1985.
10. G. Landauer, unpubl. 1979.
11. S. P. Lloyd, Binary block coding, *Bell Syst. Tech.*, **36** (1957), 517–535.
12. F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*, North Holland, Amsterdam, 1979.
13. P. Solé, The Lee association scheme, INRIA research report 591, December 1986.
14. P. Solé, Covering radius in weakly metric association schemes, INRIA research report 592, December 1986.

15. P. Solé, Rayon de recouvrement et schémas d'association, Thesis, Telecom Paris, July 1987).
16. P. Solé, Nonexistence results for perfect arithmetic codes, in preparation.
17. H. Tarnanen, Thesis, Turku University, Finland, 1982.
18. J. H. Van Lint, *Introduction to coding theory*, Springer-Verlag, Berlin–Heidelberg–New York, 1982.

Received 30 July 1987 and in revised form 20 February 1988

PATRICK SOLÉ
School of Computer and Information Science,
313 Link Hall, Syracuse University,
Syracuse, NY 13244-1240, U.S.A.